BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images may include (but are not limited to):

- BLACK BORDERS
- TEXT CUT OFF AT TOP, BOTTOM OR SIDES
- FADED TEXT
- ILLEGIBLE TEXT
- SKEWED/SLANTED IMAGES
- COLORED PHOTOS
- BLACK OR VERY BLACK AND WHITE DARK PHOTOS
- GRAY SCALE DOCUMENTS

IMAGES ARE BEST AVAILABLE COPY.

As rescanning documents *will not* correct images, please do not report the images to the Image Problem Mailbox.

CLAIMS:

1. A proactive operating environment that includes a group of proactive servers communicating over a network; each proactive server (PS_I) comprising:

a storage that includes a non erasable part that stores at least a public, non proactive related, key V^I_{Start} ; said storage further includes an erasable part for storing private and public data; said proactive server is further associated with a discardable one-time private key S^I_{Start} that corresponds to said public key V^I_{Start}; said proactive server is further associated with configuration data C;

a processor for providing at least proactive services to applications;

the proactive server is associated with a group public proactive key V_{CERT} common to said group of proactive servers and a share S^I_{CERT} of a corresponding private proactive key S_{CERT};

the processor is operative to invoke initialization procedure for generating restore related information;

the processor is further operative to invoke a restore procedure for utilizing at least said public, non proactive related, key V^I_{Start} and said restore related information for restoring at least said public proactive key V_{CERT}.

2. The system according to Claim 1, wherein said restore procedure is invoked by refresh procedure.

3. The system according to Claim 1, wherein said non erasable part of the storage being a ROM memory module.

4. The system according to Claim 1, wherein said applications being at least one of the following: Secure logging, Secure end-to-end communication, Timestamping, Certificate authority, Key recovery, Voting, Trading, Database, Operating system, Access control mechanisms, Secure Commerce.

5. The system according to Claim 1, wherein said restore related information includes restore related self information.

6. The system according to Claim 1, wherein said restore related information includes restore related others' information.

7. The system According to Claim 5, wherein said restore related self information includes $M_I = S^I_{start}(V_{Cert}, C)$.

8. The system According to Claim 6, wherein said restore related others' information includes $(S_{Cert}(M), M)$.

9. The system according to Claim 1, wherein said initialization procedure includes:

(i) input for receiving at least configuration data C, public non-proactive related key V^I_{start} and discardable one time private key S^I_{start};

(ii) the processor generating a set of keys $S_I(0)$, $V_I(0)$, $E_I(0)$, $D_I(0)$;

(iii) broadcasting said set of keys except $D_I(0)$ over the network to the rest of the servers

(1..i-1,i+1..n) in the group, so as to authenticate and encrypt the network channel;

(iv) the processor generating the group public proactive key, V_{Cert} and a share (S^I_{CERT}) of corresponding private proactive key S_{CERT};

(v) the processor generating restore related self information that includes $M_I = S^I_{start}(V_{Cert}, C)$.

(vi) discarding the one-time private key S^I_{start};

(vii) broadcasting M_I to all servers in the group, and receiving M_J from all respective SP_J servers in the group; the processor concatenating said $M_1..M_N$ so as to constrct M;

(viii) the processor generating a joint signature (S_{Cert} (M),M) that forms part of said restore related others' information; and

(ix) broadcasting the joint signature (S_{Cert} (M),M).

10. The system according to Claim 1, wherein said recover procedure includes:

(i) the processor extracting V^I_{start};

(ii) the processor extracting M_I from M;

(iii) the processor constructing V_{Cert} by applying V^I_{start} to M_I;

(iv) the processor validating M by applying V_{CERT} to the joint signature part(S_{Cert} (M); if the result matches M then the server becomes operational; sending M and S_{Cert} (M) to all the group servers;

(v) if, on the other hand, M is invalid, then waiting the receipt of another joint signature and in response repeating said (ii) to (iv).

11. For use in the system of Claim 1, an initialize procedure.

12. For use in the system of Claim 1, a restore procedure.

13. A method for providing a proactive security in proactive operating environment; the proactive operating environment includes a group of proactive servers communicating over a network; each proactive server (PS_I) comprising:

a storage that includes a non erasable part that stores at least a public, non proactive related, key V^I_{Start} ; said storage further includes an erasable part for storing private and public data; said proactive server is further associated with a discardable one-time private key S^I_{Start} that corresponds to said public key V^I_{Start}; said proactive server is further associated with configuration data C;

a processor for providing at least proactive services to applications;

the proactive server is associated with a group public proactive key V_{CERT} common to said group of proactive servers and a share S^I_{CERT} of a corresponding private proactive key S_{CERT}; the method further including:

invoking initialization procedure for generating restore related information; and invoking a restore procedure for utilizing at least said public, non proactive related, key V^I_{Start} and said restore related information for restoring at least said public proactive key V_{CERT}.

14. The method according to Claim 13, wherein said restore procedure is invoked by refresh procedure.

15. The method according to Claim 13, wherein said non erasable part of the storage being a ROM memory module.

16. The method according to Claim 13, wherein said applications being at least one of the following:

Secure logging, Secure end-to-end communication, Timestamping, Certificate authority, Key recovery, Voting, Trading, Database, Operating system, Access control mechanisms, Secure Commerce.

17. The method according to Claim 13, wherein said restore related information includes restore related self information.

18. The method according to Claim 13, wherein said restore related information includes restore related others' information.

19. The method According to Claim 17, wherein said restore related self information includes $M_I = S^I_{start}(V_{Cert}, C)$.

20. The method According to Claim 18, wherein said restore related others' information includes $(S_{Cert}(M), M)$.

21. The method according to Claim 13, wherein said initialization procedure includes:

(i) receiving at least configuration data C, public non-proactive related key V^I_{start} and discardable one time private key S^I_{start};

(ii) generating a set of keys $S_I(0)$, $V_I(0)$, $E_I(0)$, $D_I(0)$;

(iii) broadcasting said set of keys except $D_I(0)$ over the network to the rest of the servers

(*1..i-1,i+1..n*) in the group, so as to authenticate and encrypt the network channel;

(iv) generating the group public proactive key V_{Cert} and a share (S^I_{CERT}) of corresponding private proactive key S_{CERT};

(v) generating restore related self information that includes $M_I = S^I_{Start}(V_{Cert}, C)$.

(vi) discarding the one-time private key S^I_{Start};

(vii) broadcasting M_I to all servers in the group, and receiving M_J from all respective SP_J servers in the group; the processor concatenating said $M_1..M_N$ so as to constrct M;

(viii) generating a joint signature (S_{Cert} (M),M) that forms part of said restore related others' information; and

(ix) broadcasting the joint signature (S_{Cert} (M),M).

22. The method according to Claim 13, wherein said recover procedure includes:

(i) extracting V^I_{Start};

(ii) extracting M_I from M;

(iii) constructing V_{Cert} by applying V^I_{Start} to M_I;

(iv) validating M by applying V_{CERT} to the joint signature part(S_{Cert} (M); if the result matches M then the server becomes operational; sending M and S_{Cert} (M) to all the group servers;

(v) if, on the other hand, M is invalid, then waiting the receipt of another joint signature and in response repeating said (ii) to (iv).

23. For use in the method of Claim 13, an initialize procedure.

24. For use in the method of Claim 13, a restore procedure.

25. A storage medium storing computer implemented program for providing a proactive security in proactive operating environment; the proactive operating environment includes a group of proactive servers communicating over a network; each proactive server (PS_I) comprising:

a storage that includes a non erasable part that stores at least a public, non proactive related, key V^I_{Start} ; said storage further includes an erasable part for storing private and public data; said proactive server is further associated with a discardable one-time private key S^I_{Start} that corresponds to said public key V^I_{Start}; said proactive server is further associated with configuration data C;

a processor for providing at least proactive services to applications;

the proactive server is associated with a group public proactive key V_{CERT} common to said group of proactive servers and a share S^I_{CERT} of a corresponding private proactive key S_{CERT}; the method further including:

invoking initialization procedure for generating restore related information; and invoking a restore procedure for utilizing at least said public, non proactive related, key V^I_{Start} and said restore related information for restoring at least said public proactive key V_{CERT}.